# *IDOT PTC Safety Program Update*

# *Key Issues being worked on Safety Plan*

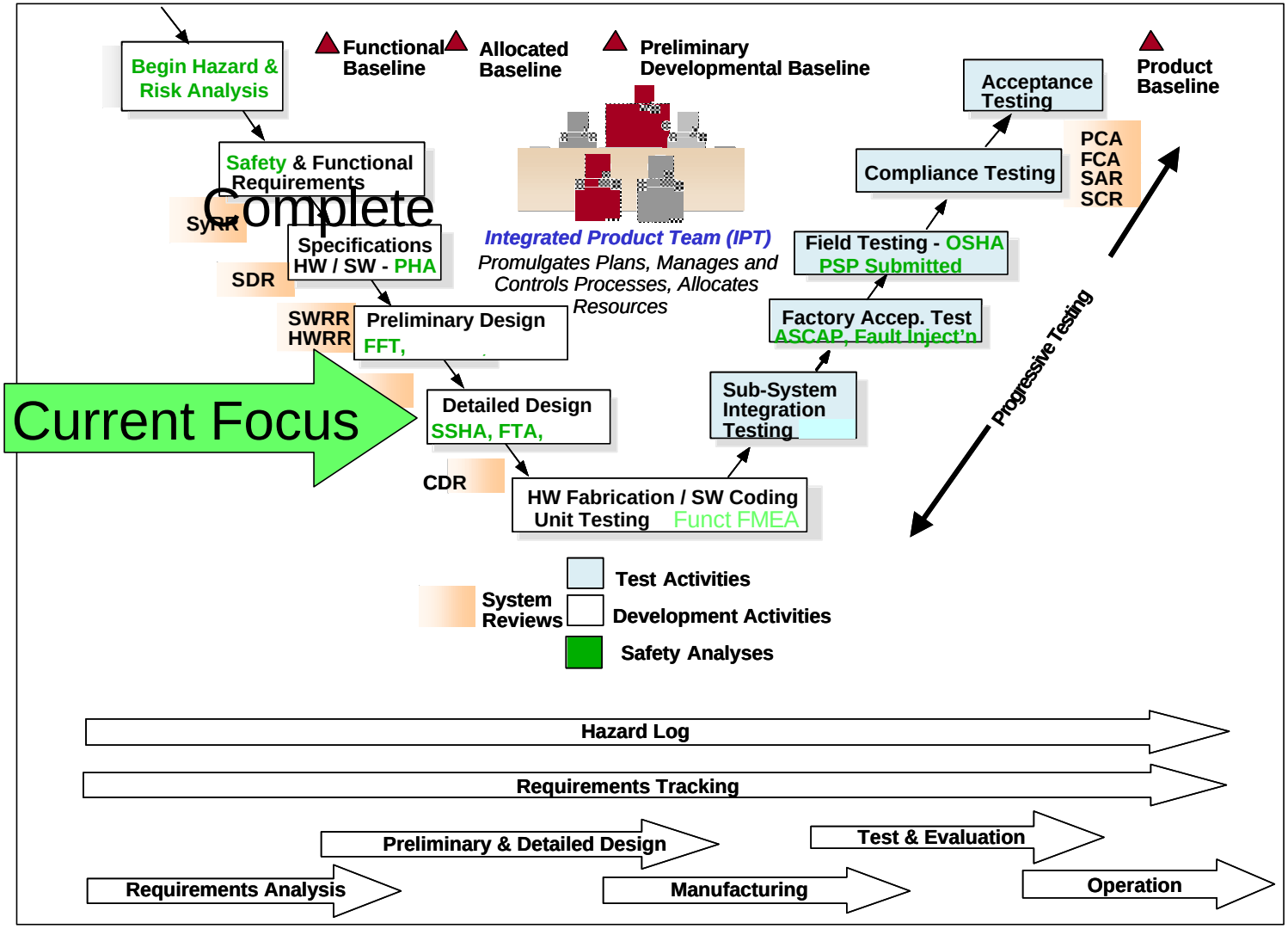
- **Incremental Safety Validation and Risk Assessment**
  - Must establish requirements and design baselines to support cost and schedule containment
  - Continue ASCAP risk assessment in final PSP
- **ASCAP base case validation activity**
  - Timetable
  - Failure rates
  - Causes of mishaps
  - Risk severity model
- **NPRM and RSPP and contract requirements comparison**

- **Core working team remains focused on Fault Tree Analysis and safety critical path**

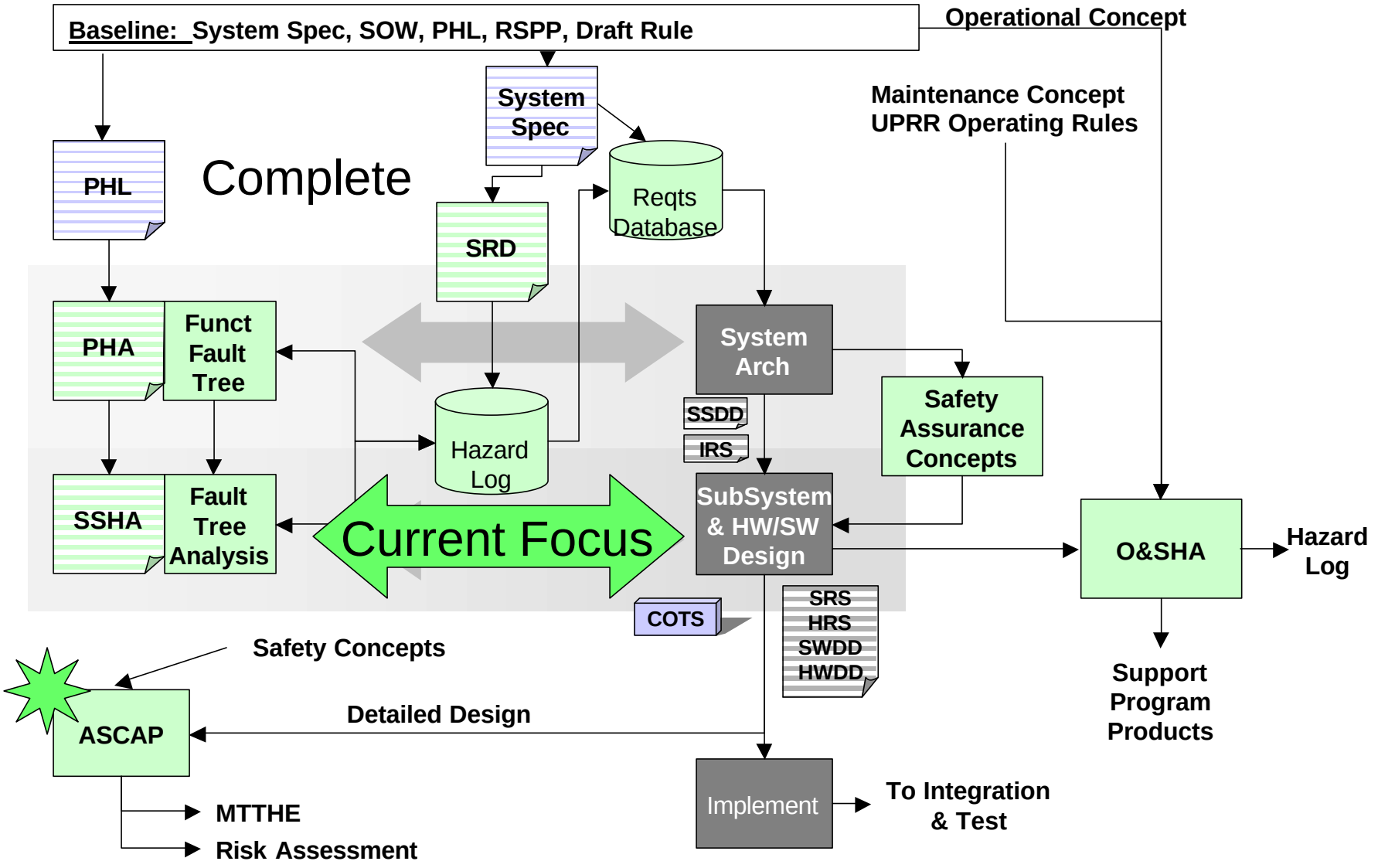
# *Purpose of Safety Plan*

- **Orchestrates the Safety Program**
- **Documents a path to completing safety analysis**
  - Clear definition of Tasks, Products and Completion Criteria
- **Simplify process of tracing safety requirements to design and test**
  - Link design to safety through req'ts and development toolset
  - Link or Integrate Databases for Safety, Design and Test
- **Improve reporting capability to demonstrate compliance**

# Program Schedule Dependencies



# Safety Analysis Process



# Safety Baseline

- **Requirements Baseline**
  - The quantitative derived requirements from the FFT takes the form of boxes in the FFT with a probability analysis to support the safety design goal.
  - The requirements baseline is established when a complete set of derived safety requirements have been written.
- **Design Baseline - The safety design is ready for CDR when:**
  - The Safety Assurance Concepts are defined
  - Verification work products SSHA, and FTA are completed
  - The Derived requirements have been allocated to system elements and the design for those elements is complete
  - The design documents (SRS, HRS, SWDD, HDD) are properly updated to include implementation of all derived safety requirements.
  - The SDI has verified the probabilities for risk against the design to determine that the design will meet the criteria that it is as safe or safer than the base case with a high degree of confidence

# Safety Verification and Validation

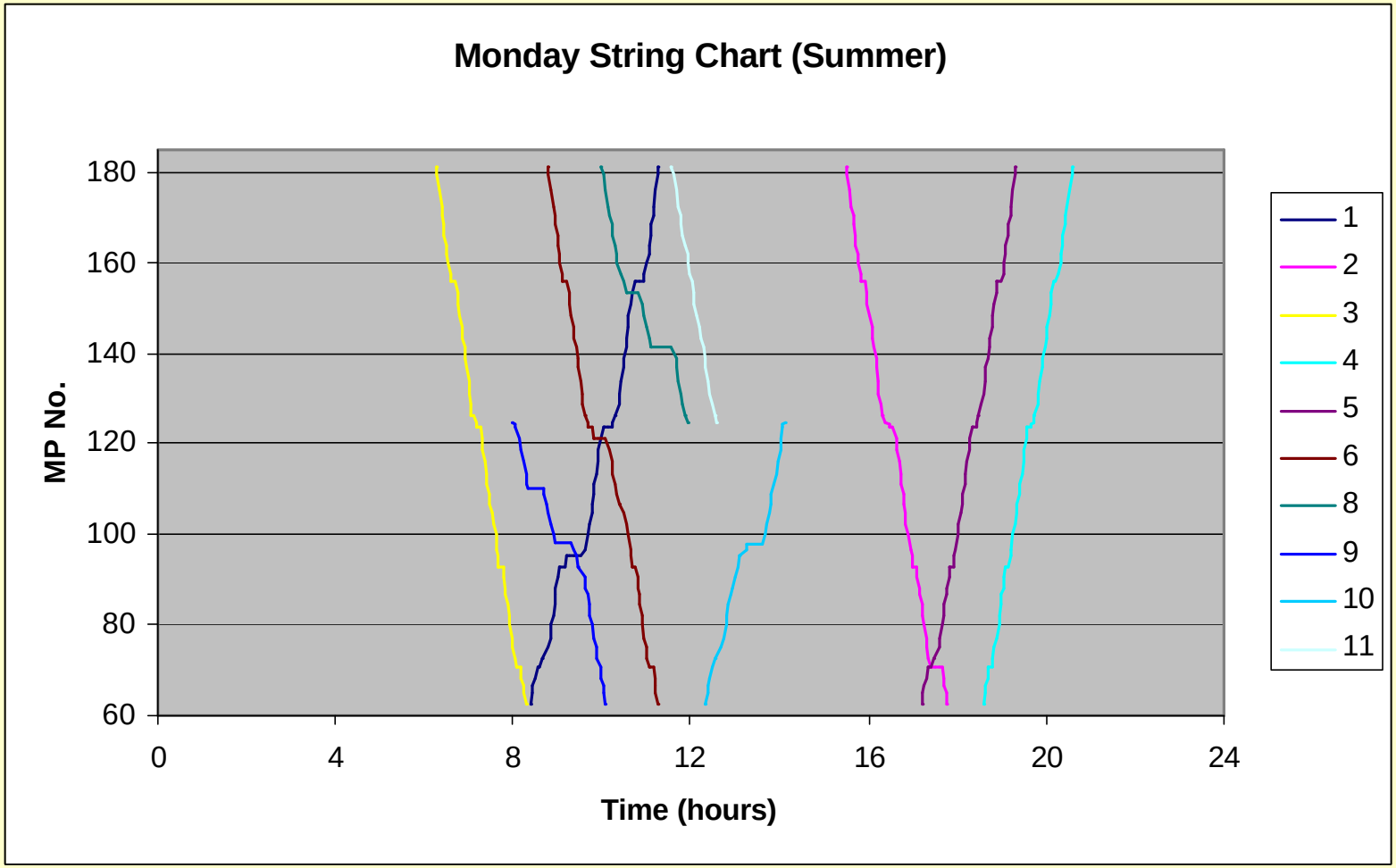
| Activity | Effect |
|---|---|
| *ASCAP will establish the base case system level likelihood of Mishap* | *When translated to probabilities, this can establish the acceptance criteria for safety.* |
| *Functional Fault Trees will allocate probabilities to mitigating functions.* | *- Establishes functional requirements baseline - Allows the SDI to proceed with development at low risk. i.e. all safety functions are defined at this point.* |
| *Fault Tree Analysis will verify the design meets target probabilities.* | *Establishes the design baseline and allows implementation to proceed. All safety design and analysis of probabilities is complete at this point. If this design is implemented correctly the system will be safe.* |
| *System Functional Testing, primarily factory testing, but some field testing where necessary, will validate the safety functions are implemented correctly.* | *PTC tested against acceptance criteria; PSP submitted based on design and preliminary test results; Final test results included in Final PSP submittal* |
| *ASCAP will provide a risk assessment of PTC* | *Final PSP will contain the ASCAP risk assessment* |

# ASCAP Way Forward

- **ASCAP model - work in process**
  - Significant progress being made; model will be updated, refined and tuned over the next 6-12 months
  - Model will be the future tool to determine risk of computer based train control systems

- **SDI proposes to use FFT's to drive design**
  - Testable Safety Requirements allocated from FTAs / FMEAs
  - FFT Probabilities verified by analysis
  - Will continue to use ASCAP for risk analysis
    - ASCAP mishaps will be analyzed to determine if PTC preventable – will be basis for likelihood comparison
    - Severity Model results will continue to evolve

# ASCAP Traffic Exposure Algorithm



# *Build 2 Acceptance*

# Overall System Test Development Approach (Build 2)

By 10/1/02

**Establish Conditions and Verification Criteria for each Build 2 SSR (per RVTM)**

| SSR | Conditions | Criteria | Lab/Fld |
|---|---|---|---|
| 1. xxxx | xxxxxxx | xxxxxxx | x |
| 2. xxxx | xxxxxxx | xxxxxxx | x |
| 3. xxxx | xxxxxxx | xxxxxxx | x |
| 4. xxxx | xxxxxxx | xxxxxxx | x |

**Establish Test Scenarios/ Title "Buckets"**

| Test Title | Scenario |
|---|---|
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |

**Define CAD/Office Integration Criteria for each CAD/Office Message**

| Message | Criteria |
|---|---|
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |
| xxxxxxx | xxxxxxxxxxxxxxxxx |

By 11/1/02

**Achieve agreement**

**Trace Matrix/RVTM Maintenance**

| SSR | Conditions | Criteria | Lab/Fld | Test ID |
|---|---|---|---|---|
| 1. xxxx | xxxxxxx | xxxxxxx | x | 1.2 |
| 2. xxxx | xxxxxxx | xxxxxxx | x | 2.3 |
| 3. xxxx | xxxxxxx | xxxxxxx | x | 1.1 |
| 4. xxxx | xxxxxxx | xxxxxxx | x | 4.4 |

**Map Verification Criteria to Test Scenario/ Title "Buckets"**

By 1/1/03

**FAT Tests**

| Test A | Test N |
|---|---|
| SSR X | SSR A |
| SSR Y | SSR B |
| SSR Z | SSR C |
| …. | …. |

**Field Tests**

| Test A | Test N |
|---|---|
| SSR X | SSR A |
| SSR Y | SSR B |
| SSR Z | SSR C |
| …. | …. |

**BQT Tests**

| Test A | Test N |
|---|---|
| SSR X | SSR A |
| SSR Y | SSR B |
| SSR Z | SSR C |
| …. | …. |

**Generate FAT Test Plans/ Procedures**

**By 2/1/03**

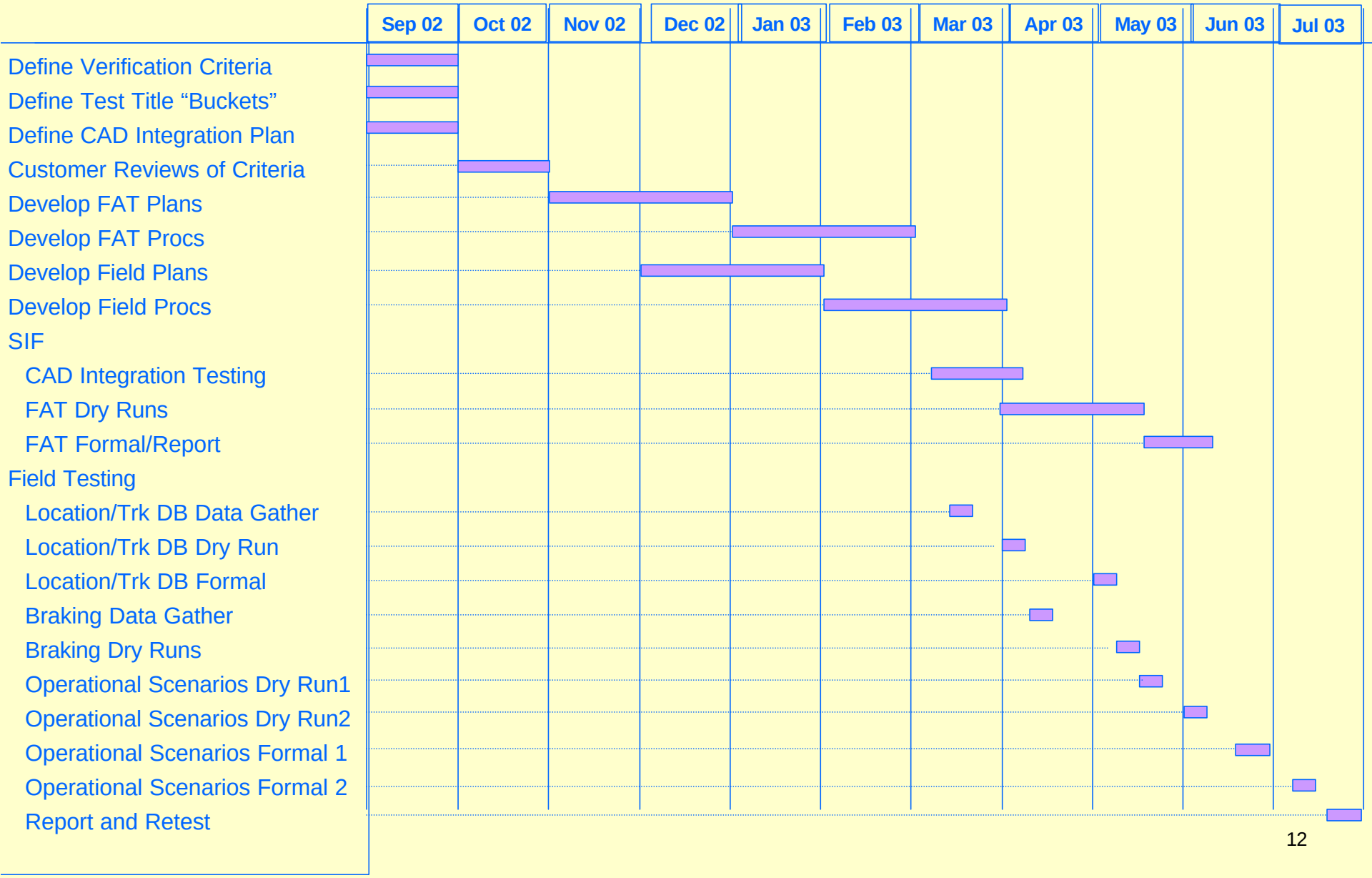
**Generate FIELD Test Plans/ Procedures**

**By 5/1/03**

**Generate BQT Test Plans/ Procedures**

**By 2/1/03**

# PTC Build 2 System Test Key Schedule Events

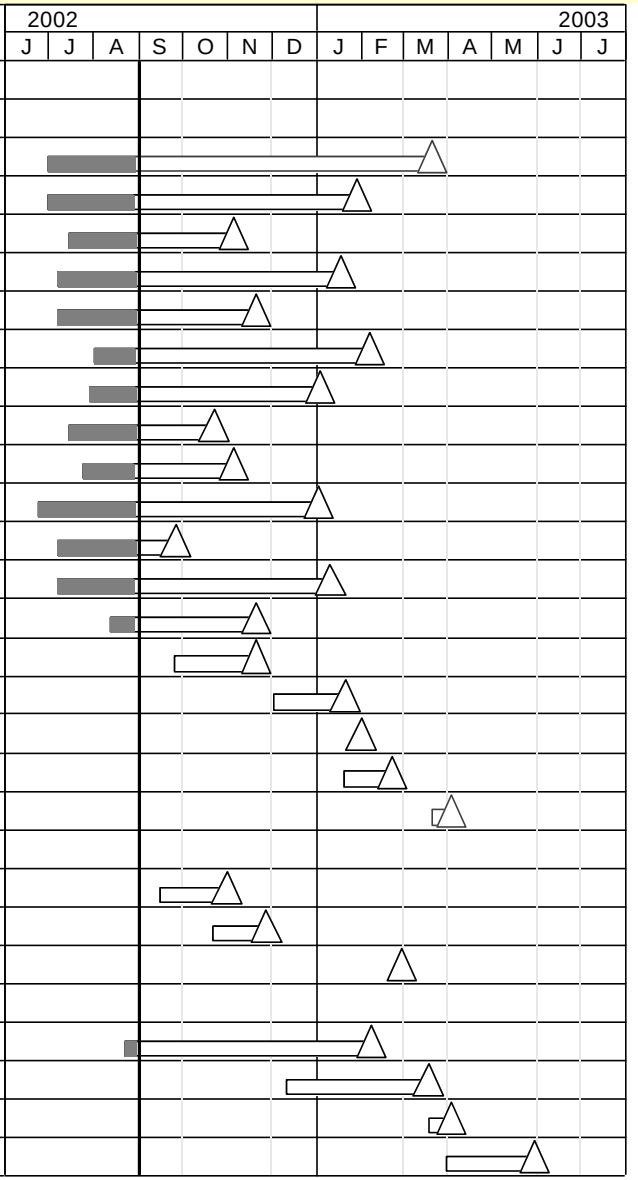


# Build 2 Key Milestones

| | |
|---|---|
| • Field BQT Completion | 01/15/03 |
| • Territory Upgrade Available (CFE) | 01/31/03 |
| • Locomotive BQT Completion | 04/03/03 |
| • Work Vehicle BQT Completion | 02/26/03 |
| • Office BQT Completion | 04/03/03 |
| • Operational CAD II Available (CFE) | 03/01/03 |
| • FAT Completion | 06/06/03 |
| • Field Test Completion | 07/30/03 |

# Build 2 Schedule

| ID | Task Name | Start | Finish |
|---|---|---|---|
| **1** | **1 Build 2 Schedule** | Mon 9/10/01 | Wed 7/30/03 |
| **2** | **1.1 Office Development** | Mon 6/24/02 | Thu 4/3/03 |
| 3 | 1.1.1 Authority Manager Design/Code/Unit Test | Mon 7/1/02 | Fri 3/21/03 |
| 4 | 1.1.2 Speed Manager Design/Code/Unit Test | Mon 7/1/02 | Tue 1/28/03 |
| 5 | 1.1.3 Enforcement Manager Design/Code/Unit Test | Mon 7/15/02 | Tue 11/5/02 |
| 6 | 1.1.4 Advisory Manager Design/Code/Unit Test | Mon 7/8/02 | Fri 1/17/03 |
| 7 | 1.1.5 Train Manager Design/Code/Unit Test | Mon 7/8/02 | Wed 11/20/02 |
| 8 | 1.1.6 Track Data Manager Design/Code/Unit test | Fri 8/2/02 | Thu 2/6/03 |
| 9 | 1.1.7 Location Manager Design/Code/Unit Test | Tue 7/30/02 | Fri 1/3/03 |
| 10 | 1.1.8 Dispatch/I/O Design/Code/Unit Test | Mon 7/15/02 | Tue 10/22/02 |
| 11 | 1.1.9 Segment I/O Design/Code/Unit Test | Thu 7/25/02 | Tue 11/5/02 |
| 12 | 1.1.10 Pacing Design/Code/Unit Test | Mon 6/24/02 | Thu 1/2/03 |
| 13 | 1.1.11 Work Vehicle Manager Design/Code/Unit Test | Mon 7/8/02 | Thu 9/26/02 |
| 14 | 1.1.12 Wayside Manager Design/Code/Unit test | Mon 7/8/02 | Fri 1/10/03 |
| 15 | 1.1.13 User Interface Design/Code/Unit Test | Tue 8/13/02 | Wed 11/20/02 |
| 16 | 1.1.14 Office Simulation | Thu 9/26/02 | Wed 11/20/02 |
| 17 | 1.1.15 Office Software Integration (SWIT) | Tue 12/3/02 | Mon 1/20/03 |
| 18 | 1.1.16 Initial Drop to Integration and Test | Fri 1/31/03 | Fri 1/31/03 |
| 19 | 1.1.17 BQT Dry Runs | Mon 1/20/03 | Fri 2/21/03 |
| 20 | 1.1.18 BQT Final | Fri 3/21/03 | Thu 4/3/03 |
| **21** | **1.2 Build 2 CDR** | Mon 9/16/02 | Wed 11/27/02 |
| 22 | 1.2.1 Object Reviews | Mon 9/16/02 | Thu 10/31/02 |
| 23 | 1.2.2 System Level Reviews | Tue 10/22/02 | Wed 11/27/02 |
| **24** | **1.3 CAD (CFE)** | Sat 3/1/03 | Sat 3/1/03 |
| **25** | **1.4 Locomotive Software Development** | Fri 8/23/02 | Fri 5/30/03 |
| 26 | 1.4.1 Design/Code/Unit Test | Fri 8/23/02 | Fri 2/7/03 |
| 27 | 1.4.2 CIT/SIT/CSCI Integration | Wed 12/11/02 | Tue 3/18/03 |
| 28 | 1.4.3 BQT Dry Runs/BQT | Wed 3/19/03 | Thu 4/3/03 |
| 29 | 1.4.4 Braking/Location Field Testing | Tue 4/1/03 | Fri 5/30/03 |



# Build 2 Schedule

| ID | Task Name | Start | Finish |
|---|---|---|---|
| **30** | **1.5 Work Vehicle Software Vehicle Development** | Thu 7/25/02 | Wed 2/26/03 |
| 31 | 1.5.1 Design/Code/Unit Test | Thu 7/25/02 | Mon 1/6/03 |
| 32 | 1.5.2 CIT/SIT/CSCI Integration | Tue 1/7/03 | Tue 2/11/03 |
| 33 | 1.5.3 BQT Dry Runs/BQT | Wed 2/12/03 | Wed 2/26/03 |
| **34** | **1.6 Field Development** | Mon 9/10/01 | Wed 1/15/03 |
| 35 | 1.6.1 Design/Code/Unit Test less Defect Detectors | Mon 9/10/01 | Wed 5/1/02 |
| 36 | 1.6.2 Equipment Shipped | Wed 1/2/02 | Tue 8/27/02 |
| 37 | 1.6.3 BQT Dry Runs/BQT | Fri 11/29/02 | Wed 1/15/03 |
| **38** | **1.7 FAT** | Mon 4/7/03 | Fri 6/6/03 |
| 39 | 1.7.1 FAT Dry Runs | Mon 4/7/03 | Fri 5/2/03 |
| 40 | 1.7.2 FAT Final Rehearsal | Mon 5/5/03 | Fri 5/16/03 |
| 41 | 1.7.3 Formal FAT | Mon 5/19/03 | Fri 5/30/03 |
| 42 | 1.7.4 FAT Data Analysis | Thu 5/22/03 | Fri 6/6/03 |
| 43 | 1.7.5 Submit FAT Test Report | Tue 5/27/03 | Fri 6/6/03 |
| **44** | **1.8 Field Compliance/Acceptance Test** | Mon 6/2/03 | Wed 7/30/03 |
| 45 | 1.8.1 Field Dry Run Rehearsal | Mon 6/2/03 | Wed 6/18/03 |
| 46 | 1.8.2 Formal Field Test | Thu 6/19/03 | Thu 7/10/03 |
| 47 | 1.8.3 Data Analysis | Fri 6/27/03 | Mon 7/14/03 |
| 48 | 1.8.4 Retest period | Fri 7/11/03 | Fri 7/18/03 |
| 49 | 1.8.5 Test Report and System Acceptance | Thu 6/26/03 | Wed 7/30/03 |
| **50** | **1.9 PSP** | Thu 7/18/02 | Wed 7/30/03 |
| 51 | 1.9.1 PSP Draft | Thu 7/18/02 | Fri 5/30/03 |
| 52 | 1.9.2 PSP Final | Mon 6/2/03 | Wed 7/30/03 |
| **53** | **1.10 Training** | Tue 2/11/03 | Wed 7/30/03 |
| **54** | **1.11 Equipping Remaining Trains** | Tue 4/1/03 | Thu 5/15/03 |
| 55 | 1.11.1 UPRR (4) Installed and Operational | Tue 4/1/03 | Tue 4/1/03 |
| 56 | 1.11.2 UPRR (2) Equipment Delivered for Installation | Thu 5/15/03 | Thu 5/15/03 |
| 57 | 1.11.3 Amtrak (7) Equipment Delivered for Installation | Thu 5/15/03 | Thu 5/15/03 |